1. **SEIZURE AND PROCESSING OF ELECTRONIC STORAGE DEVICES AND DIGITAL EVIDENCE**

A. Only employees who are authorized by the Digital Forensics Investigative Unit (DFIU) or Internet Crimes Against Children (ICAC) task force may seize and process electronic storage devices and digital evidence. Electronic storage devices include but are not limited to:

- Computers
- Cell phones, tablets, or other hand-held devices
- Hard disc drives
- Blue Ray discs
- Digital video discs (DVDs)
- Flash memory devices
- Memory cards
- Tapes

NOTE: Electronic storage devices and digital evidence as outlined in this section do not include video surveillance systems which are the responsibility of FIU (see section 10 of this order for more information).

B. Officers who are not authorized by DFIU or ICAC and encounter electronic storage devices that may have been used to facilitate the commission of a crime will contact the VCB desk sergeant for triaging and to be routed to the DFIU or ICAC standby supervisor.

- Officers **will** not attempt to access, review, or search the contents of any device prior to examination by a DFIU certified examiner or other authorized employee outside of a public safety emergency.

  * When the risk to public safety is such that an immediate warrantless search is necessary, the DFIU or ICAC standby supervisor should be contacted for assistance in minimizing potential evidence issues.

C. Prior to seizing any electronic storage device, employees will ensure there is legal authority to collect the evidence (search warrant, etc.).

- Evidence will be impounded in accordance with established procedures and policies as outlined in Operations Order 5.8.00, Evidence, Impounding, and Property.

  * Unless otherwise directed by DFIU, the seizing employee will ensure all physical evidence is impounded.
  * Each electronic storage device must have a separate barcode.

D. When electronic storage devices/digital evidence has been seized and the investigating detective determines an examination is necessary, a Digital Forensic Processing Request will be completed by accessing the DFIU PolicePoint page.

NOTE: Prior to submitting the Digital Forensic Processing Request, ensure each electronic storage device is in its own evidence bag with a barcode (evidence bags containing numerous devices/barcodes will not be processed until separated and given individual barcodes).

EXCEPTION: When written or audio recorded verbal consent has been given to examine a device, the device will not be impounded; however, it will be placed in a property bag with the IR number written on it (do not generate a barcode) (see section 24.E.(2)(a)(ii) below for more information).

(1) Each field with an asterisk (*) on the Digital Forensic Processing Request will be completed and should provide as much information as possible.

- The request should specifically indicate what information (photos, videos, texts, short message service (SMS), multi-media service (MMS), etc.) is needed to further the investigation, to include date ranges.

1. D. (2) A DFIU examiner will obtain the evidence from PMB and re-impound upon completion of the examination.

- The DFIU examiner will notify the investigating detective of the expected start date for the examination (completion time will vary depending on the volume of data and complexity of the system).

E. Prioritizing Evidence Processing/Examinations

(1) Digital forensic evidence will be triaged by an DFIU examiner to ensure the queue is maintained and to prioritize the processing/examination of electronic storage devices.

(a) Devices which require immediate attention will be determined daily by the on-call DFIU examiner.

- Immediate attention is warranted when all reasonable leads have been exhausted and a need for known evidence exists on a device.

(b) All other devices will follow the priority-based system outlined below in section 24.F.(2) of this order.

(2) Priority-Based System

(a) PRIORITY 1 (P1) - EMERGENCY PROCESSING/SAME-DAY CONSENT	
(i) General Information	• Devices which are found OFF, then powered ON, **WILL NOT** be considered as a powered-on device.
(ii) Victim/ Witness Consent	• Phones and related devices which require same day processing require a WRITTEN consent or audio recorded VERBAL consent. • During business hours, bring the consent, device, and if needed, the passcode, to examiners at 620 West Washington for assistance. • If after hours and weekend assistance is needed, contact the VCB desk for the on-call examiner.
(iii) After First Unlock (AFU) (Powered ON Apple and Android Phones)	• When a locked phone has known critical evidence on it, the DFIU supervisor will be contacted. • Locked phones must remain powered on, charged with the subscriber identity module (SIM) card removed, and brought to examiners at 620 West Washington as soon as practical.
(iv) Computer Systems (Computers/ Laptops/Tablets and Related Devices)	• When there is an incident involving any type of computer or laptop (powered On or OFF) in which there is possible evidence and the collection of the digital evidence is needed, the DFIU supervisor should be contacted.
(b) PRIORITY 2 (P2) - ELEVATED PRIORITIZATION	
(i) General Information	• Digital forensic evidence which needs to be processed/examined in a shorter time frame, however, it does not meet the P1 criteria. • If articulable factors exist (not beliefs or suspicions) which necessitate P2 processing (generally on a next-day to seven-day time frame), the DFIU supervisor will be contacted. • Review the below criteria to determine if the device warrants P2 processing/examination. * Impound all devices and submit a Digital Forensic Processing Request by accessing the DFIU PolicePoint page.
(ii) Exigency of Evidence	• Known evidence on a device is needed for any reason other than probable cause. • Possible evidence is on a device.
(iii) Status of Device	• Powered On - Any device that is found powered ON with a passcode, but it does not meet the P1 requirements. • Powered Off - Any device found powered OFF with no passcode available.

1. E. (2) Priority-Based System (continued)

(c) PRIORITY 3 (P3) - STANDARD PRIORITIZATION	
(i) General Information	• Any device with no known evidence and is powered OFF, has no passcode available, or is severely damaged, will be considered a P3 and will be processed when assigned and completed as permitted.
NOTE: For any questions regarding prioritization, contact the VCB desk sergeant to be routed to the DFIU standby supervisor	

F. Rule 15 (Discovery)

- The investigating detective is responsible for maintaining a copy of all reports generated regarding a digital request (includes, but is not limited to, Cellebrite Reader reports, Axiom portable cases, and Griffeye reports).

G. Maricopa County Attorney Office (MCAO) Discovery Requests

- When MCAO asks for evidence that the investigating detective cannot access, advise MCAO to email DFIU directly to facilitate the request.

H. Digital Forensic Evidence Storage - All digital forensic evidence acquired during the course of a criminal or administrative investigation must be imaged and permanently archived by an authorized digital evidence examiner.

- The primary image of the digital evidence will be maintained in secure long-term storage within ACTIC, in agreement with DPS and in accordance with DFIU procedures.
- A working copy of the digital evidence will be provided to investigators via approved data transfer methods.
    - Investigators will ensure the working copy and/or specific items of digital evidence are made available for discovery and/or impounded as necessary.

NOTE: The use of external hard drives, thumb drives, DVDs, and Blue Ray discs are **not** acceptable forms of permanent storage.